

Appln. No.: 09/930,903
 Amdt. Dated February 14, 2005
 Reply to Office Action dated October 14, 2004

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Canceled)
2. (Canceled)
3. (Canceled)
4. (Canceled)
5. (Canceled)
6. A method for sending ~~an encrypted~~ message, said method comprising the steps of:
 - a) generating by a sender a password P;
 - b) sending the password P to a message recipient over a first channel;
 - c) generating authentication information by the sender for server authentication of the message recipient;
 - ad) generating by the sender a random number as an initialization vector IV4;
 - be) generating by the sender a private key PK as $H(IV4 \parallel P)$, where P is a password known to a message recipient;
 - e)f) generating by the sender an encryption $ENC = E(M \parallel H(M), PK)$, where E is a predetermined symmetric key encryption algorithm, M is the message and H() is an agreed upon hashing algorithm; and
 - eg) sending the authentication information and (IV4, ENC) from the sender to said message recipient the server over a second channel;
 - h) authenticating the message recipient over a third channel using the information;

Appl. No.: 09/930,903
 Amdt. Dated February 14, 2005
 Reply to Office Action dated October 14, 2004

l) sending ENC from the server to the message recipient over the third channel only when the message recipient has been authenticated by the server.

7. A method as described in claim 6 comprising the further step of receiving authentication of said message recipient prior to sending (IV4, ENC).

8. A method as described in claim 7-6 where said message recipient is authenticated by the steps of:

- ~~a) generating a password P;~~
- ~~b) sending said password P to said message recipient over a first, secure channel;~~
- ea) generating by the sender a first random number as a first initialization vector IV1;
- eb) generating by the sender $H(IV1 \parallel P)$ as an authentication key AK;
- ec) generating by the sender an authentication string AS as $E(ACNST1, AK)$, where ACNST1 is a predetermined constant and E is a predetermined symmetric key encryption algorithm;
- d) sending IV1 and AS to the server over the second channel
- ~~fe) generating by the server a second random number as a second initialization vector IV2;~~
- gf) sending from the server said vectors IV1 and IV2 to said message recipient over a the second-third channel;
- g) generating by the message recipient a third random number as a third initialization vector IV3;
- h) regenerating by the message recipient the authentication key AK;
- i) regenerating by the message recipient the authentication string AS;
- ~~h) receiving a third random number as a third initialization vector IV3 and an authentication response AR from said recipient over said second channel;~~
- ij) generating by the message recipient an authentication response key ARK as $H(IV2 \parallel IV3 \parallel AS)$;

Appln. No.: 09/930,903
Amdt. Dated February 14, 2005
Reply to Office Action dated October 14, 2004

k) generating by the message recipient the authentication response AR as $E(\text{ACNST2}, \text{ARK})$, where ACNST2 is a predetermined constant and E is a predetermined symmetric key encryption algorithm;

l) sending from the recipient to the server IV3 and AR;

m) regenerating by the server the authentication response key ARK as $H(\text{IV2} \parallel \text{IV3} \parallel \text{AS})$;

in) generating-computing by the server a decryption $D(\text{AR}, \text{ARK})$, where D is a symmetric decryption algorithm corresponding to E; and

ko) authenticating said message recipient only if $D(\text{AR}, \text{ARK}) = \text{ACNST2}$, where ACNST2 is a second predetermined constant.

9.. (Canceled)

10. A method as described in claim 6 where H is an encryption algorithm defined hash algorithm using said encryption algorithm E.

11. A method as described in claim 10 where said encryption algorithm is expressed in less than 1000 bytes of code; whereby software comprising said algorithm can be quickly downloaded to a user's system.

12. A method as described in claim 11 where said encryption algorithm is an RC4 algorithm.

13. (Canceled)

14. (Canceled)

15. (Canceled)

16. (Canceled)

17. (Canceled)

Appln. No.: 09/930,903
Amdt. Dated February 14, 2005
Reply to Office Action dated October 14, 2004

18. A method for receiving an encrypted message that was originally sent by a sender to a server over a second channel, said method comprising the steps of:

a) receiving (IV4, ENC) from a server over a third channel, where $ENC = E(M \parallel H(M), PK)$, M is said message, and E is a predetermined encryption algorithm, IV4 is a random number as an initialization vector, and H() is an agreed upon hashing algorithm;

b) generating PK as $H(IV4 \parallel P)$, where P is a password received from a the sender of said message over a secure-first channel;

c) generating $D(ENC, PK) = (M \parallel H(M))$, where D is a symmetric key decryption algorithm corresponding to E;

d) calculating H(M) from said value of M generated in step c; and

e) accepting said generated value of M only if said calculated value of H(M) equals said value of H(M) generated in step c.

19. A method as described in claim 18 where H is an encryption algorithm defined hash algorithm using said encryption algorithm E.

20. A method as described in claim 19 where said encryption algorithm is expressed in less than 1000 bytes of code; whereby software comprising said algorithm can be quickly downloaded to a user's system.

21. A method as described in claim ~~16~~19 where said encryption algorithm is an RC4 algorithm.

22. A method as described in claim 18 where said initialization vector IV4 and said encryption ENC are received from said sender through a server.

23. (Canceled)

Appln. No.: 09/930,903
Amdt. Dated February 14, 2005
Reply to Office Action dated October 14, 2004

- 24. (Canceled)
- 25. (Canceled)
- 26. (Canceled)
- 27. (Canceled)
- 28. (Canceled)
- 29. (Canceled)
- 30. (Canceled)
- 31. (Canceled)
- 32. (Canceled)
- 33. (Canceled)
- 34. (Canceled)
- 35. (Canceled)
- 36. (Canceled)